PERGAMON Computers and Mathematics with Applications 41 (2001) 1473–1474

An International Journal
computers & mathematics with applications

www.elsevier.nl/locate/camwa

Letter to the Editor,* Regarding "Powersums Representing Residues $\bmod p^k$, from Fermat to Waring"

R. J. CHAPMAN
School of Mathematical Sciences
University of Exeter, Exeter, EX4 4QE, U.K.
rjc@maths.ex.ac.uk

I refer to the paper "Powersums representing residues $\bmod p^k$, from Fermat to Waring" by N. F. Benschop, published recently in *Computers and Mathematics with Applications*, Vol. 39, pp. 253–261, (2000).

I have two comments to make. The argument given by the author as a proof of Theorem 3.1 is erroneous, and Theorem 3.2 is a straightforward consequence of a result published in 1969.

I quote Theorem 3.1:

"If $r > 1$ divides $p^2 - 1$, then $r^p \neq r \bmod p^k$ $(k \geq 3)$."

Here p is understood to be an odd prime number; also it should be noted that the author uses the equals sign in congruences rather than the more usual symbol $\equiv$.

To discuss the author's argument I need to summarize some of his definitions and notations. He uses Z_k for the ring of integers modulo p^k (p is a fixed odd prime), G_k for the multiplicative group of units of Z_k (so that $|G_k| = (p-1)p^{k-1}$) and denotes the unique subgroups of orders $p-1$ and p^{k-1} of G_k as A_k and B_k, respectively. He calls the subgroup A_k the *core*; it is characterized as the set of $r \in G_k$ with $r^{p-1} \equiv 1 \pmod{p^k}$, while B_k consists of the residues in G_k congruent to 1 modulo p. He correctly asserts that G_k is the internal direct product of A_k and B_k, that is, each element of G_k can be uniquely written as a product of an element of A_k with one of B_k.

To turn to the claimed proof, the author begins by correctly noting that it suffices to consider the case where $k = 3$. He then writes $p^2 - 1 = rs$ so that s is also a positive integer, and points out that r and $-s$ are inverses when considered in the group G_2, and so have equal order as elements of that group. (This does not seem to be of importance in the sequel.)

He now considers the group G_3, correctly asserting that $rs = p^2 - 1$ is not an element of A_3 and so at most one of r and s can lie in A_3. Also he notes that $(rs)^p \equiv -1 \pmod{p^3}$; hence, r^p and $-s^p$ are inverses in G_3 and so have the same order in that group. He then claims that neither of r^{p-1} and s^{p-1} are congruent to 1 modulo p^k citing the final paragraph of his argument as justification.

This paragraph contains the crucial error. The author uses the direct product decomposition of G_3 as $A_3 \times B_3$ to write each $n \in G_3$ uniquely as $n'n''$ where $n' \in A_3$ and $n'' \in B_3$. He

*Letters to the Editor are not refereed before publication.

PII: S0898-1221(01)00110-9

correctly asserts that since r^p and $-s^p$ are inverses in G_3, it follows that $(r^p)''$ and $(-s^p)''$ are inverses in B_3. Thus $(r^p)''$ and $(-s^p)''$ have the same order in B_3 which must divide p^2, the order of B_3. He then claims that this common order cannot be 1 ("and discarding order 1 ... their common order is p or p^2"). But this common order can be 1. For example, let $p = 11$ and $r = 3$. Then $s = 40$ and $r^p = 3^{11} \equiv 124 \pmod{11^3}$. One then checks that $124^{10} \equiv 1 \pmod{11^3}$ so that $124 \in A_3$. Thus $(3^{11})'' \equiv (124)'' \equiv 1 \pmod{11^3}$ contrary to the author's assertion. The author then relies on the supposition that $(r^p)''$ cannot have order 1 to deduce first that r^p has order divisible by p in G_3 and then that r has order divisible by p in G_3. As $r^{p-1} \not\equiv 1 \pmod{p^3}$ is equivalent to p dividing the order of r in G_3, this, if true, would yield the desired conclusion.

As this attempted proof relies on an intermediate statement which is false (having a counterexample) then it is invalid. Unfortunately, I see no way of plugging the gap in this proof. To my knowledge, no results of this nature have been proved before in the literature.

Theorem 3.2 is is a simple consequence of the Theorem in [1]. Bhaskaran proves that each p-adic integer is the sum of four p^{th} powers of p-adic integers. It follows immediately that each residue modulo p^2 is the sum of at most four elements of A_2. By including terms $1^p + (-1)^p$ as necessary (we are assuming that p is odd), one can represent each residue modulo p^2 as the sum of three or four elements of A_2. This establishes the $k = 2$ case of Theorem 3.2, which as the author correctly points out is sufficient to establish it for all $k \geq 2$.

REFERENCES

1. M. Bhaskaran, Sums of p^{th} powers in a P-adic ring, *Acta Arith.* **XV**, 217–219 (1969).